



FortiSIEM - ESX Installation and Migration Guide

Version 6.1.1

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



10/04/2023

FortiSIEM 6.1.1 ESX Installation and Migration Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Set Network Time Protocol for ESX	6
Import FortiSIEM into ESX	7
Edit FortiSIEM Hardware Settings	13
Start FortiSIEM from the VMware Console	14
Configure FortiSIEM via GUI	15
Upload the FortiSIEM License	19
Choose an Event Database	19
Cluster Installation	20
Install Supervisor	20
Install Workers	21
Register Workers	22
Install Collectors	23
Register Collectors	24
Installing on ESX 6.5	26
Importing a 6.5 ESX Image	27
Resolving Disk Save Error	28
Adding a 5th Disk for /data	30
Migrating from FortiSIEM 5.3.x or 5.4.0	31
Pre-Migration Checklist	31
Migrate All-in-one Installation	35
Download the Bootloader	35
Prepare the Bootloader	36
Load the FortiSIEM 6.1.1 Image	37
Prepare the FortiSIEM VM for 6.1.1	39
Migrate to FortiSIEM 6.1.1	44
Finishing Up	48
Migrate Cluster Installation	48
Delete Workers	48
Migrate Supervisor	49
Install New Worker(s)	49
Register Workers	49
Set Up Collector-to-Worker Communication	49
Working with Pre-6.1.0 Collectors	49
Install 6.1.1 Collectors	49
Register 6.1.1 Collectors	50

Change Log

Date	Change Description
09/05/2018	Initial version of FortiSIEM - ESX Installation Guide.
03/29/2019	Revision 1: updated the instructions for registering the Collector on the Supervisor node.
05/22/2019	Revision 2: added a note regarding VMotion support.
11/20/2019	Release of FortiSIEM - ESX Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM - ESX Installation Guide for 5.3.0.
08/15/2020	Revision 3: Updated deployment and installation for FortiSIEM 6.1.0 on VMware ESX.
11/03/2020	Revision 4: Updated deployment and installation for FortiSIEM 6.1.1 on VMware ESX.
02/04/2021	Revision 5: Updated Migration content.
02/16/2021	Revision 6: Added Installing on ESX 6.5 content to 6.1.1.
02/23/2021	Revision 7: Minor update to Pre-Migration Checklist.
03/18/2021	Revision 8: Minor update to Pre-Migration Checklist for 6.1.1.
03/29/2021	Revision 9: Minor update to Pre-Migration Checklist for 6.1.1.
04/21/2021	Revision 10: Added Installing on ESX 6.5 content to 6.2.0. Minor update to Pre-Installation Checklist to 6.1.1 and 6.2.0.
04/22/2021	Revision 11: Added Installing on ESX 6.5 content to 6.1.0. Minor update to Pre-Installation Checklist to 6.1.0.
04/28/2021	Revision 12: Updated Pre-Installation Checklist for 6.1.0, 6.1.1 and 6.2.0.
11/19/2021	Revision 13: Updated Register Collectors section for 6.1.x guides.
08/18/2022	Revision 14: Updated All-in-one Installation section.
10/20/2022	Revision 15: Updated Register Collectors instructions for 6.x guides.

Fresh Installation

- [Pre-Installation Checklist](#)
- [All-in-one Installation](#)
- [Cluster Installation](#)
- [Installing on ESX 6.5](#)

Pre-Installation Checklist

Before you begin, check the following:

- Release 6.1.1 requires at least ESX 6.5, and ESX 6.7 Update 2 is recommended. To install on ESX 6.5, see [Installing on ESX 6.5](#).
- Ensure that your system can connect to the network. You will be asked to provide a DNS Server and a host that can be resolved by the DNS Server and responds to ping. The host can either be an internal host or a public domain host like google.com.
- Deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
 - All-in-one with Supervisor only, or
 - Cluster with Supervisor and Workers
- Storage type
 - Online – Local or NFS or Elasticsearch
 - Archive – NFS or HDFS
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB

Node	vCPU	RAM	Local Disks
Workers	Minimum – 8	Minimum – 16GB	OS – 25GB
	Recommended - 16	Recommended – 24GB	OPT – 100GB
Collector	Minimum – 4	Minimum – 4GB	OS – 25GB
	Recommended – 8 (based on load)	Recommended – 8GB	OPT – 100GB

Note: compared to FortiSIEM 5.x, you need one more disk (OPT) which provides a cache for FortiSIEM.

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Before proceeding to FortiSIEM deployment, you must configure the external storage.

- For NFS deployment, see *FortiSIEM - NFS Storage Guide* [here](#).
- For Elasticsearch deployment, see *FortiSIEM - Elasticsearch Storage Guide* [here](#).

All-in-one Installation

This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

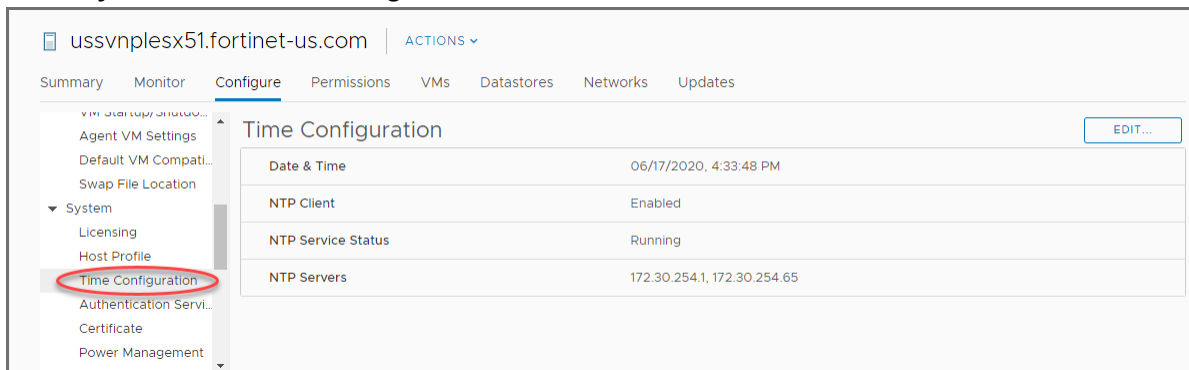
- [Set Network Time Protocol for ESX](#)
- [Import FortiSIEM into ESX](#)
- [Edit FortiSIEM Hardware Settings](#)
- [Start FortiSIEM from the VMware Console](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

Set Network Time Protocol for ESX

FortiSIEM needs accurate time. To do this you must enable NTP on the ESX host which FortiSIEM Virtual Appliance is going to be installed.

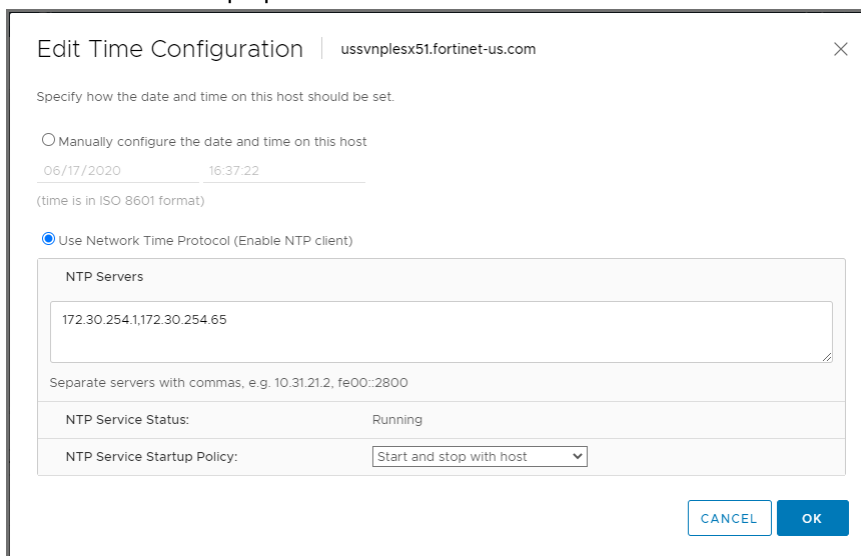
1. Log in to your VCenter and select your ESX host.
2. Click the **Configure** tab.

3. Under **System**, select **Time Configuration**.



4. Click **Edit**.

5. Enter the time zone properties.



6. Enter the IP address of the NTP servers to use.

If you do not have an internal NTP server, you can access a publicly available one at <http://tf.nist.gov/tf-cgi/servers.cgi>.

7. Choose an **NTP Service Startup Policy**.

8. Click **OK** to apply the changes.

Import FortiSIEM into ESX

1. Go to the Fortinet Support website <https://support.fortinet.com> to download the ESX package `FSM_FULL_ALL_ESX_6.1.1_Build0118.zip`. See [Downloading FortiSIEM Products](#) for more information on downloading products from the support website.
2. Uncompress the packages for Super/Worker and Collector (using [7-Zip tool](#)) to the location where you want to install the image. Identify the `.ova` file.
3. Right-click on your own host and choose **Deploy OVF Template**. The Deploy OVA Template dialog box appears.
4. In **1 Select an OVF template** select **Local file** and navigate to the `.ova` file. Click **Next**. If you are installing from a URL, select **URL** and paste the OVA URL into the field beneath **URL**.

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template
Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☒ URL

<http://engnas.accelops.net/pub/builds/6.1.1/FortiSIEM-VA-6.1.1.0118.ova>

☐ Local file

No file chosen

5. In **2 Select a Name and Folder**, make any needed edits to the **Virtual machine name** field. Click **Next**.

Deploy OVF Template

✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder
Specify a unique name and target location

Virtual machine name: FortiSIEM-VA-6.1.1.0118

Select a location for the virtual machine.

vc-devops.fortinet-us.com

US-NPL

6. In **3 Select a compute resource**, select any needed resource from the list. Click **Next**.

Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a compute resource
Select the destination compute resource for this operation

US-NPL

NPL

NPL-MGMT

7. Review the information in **4 Review details** and click **Next**.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Ready to complete

Review details

Verify the template details.

Publisher	FortiSIEM-SelfSigned (Untrusted certificate)
Product	FortiSIEM-VA
Version	6.1.1.0118
Vendor	Fortinet, Inc.
Download size	3.8 GB
Size on disk	5.7 GB (thin provisioned)
	25.0 GB (thick provisioned)

8. **5 License agreements**. Click **Next**.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Ready to complete

Fortinet Product License Agreement / EULA and Warranty Terms

Trademarks and Copyright Statement

Fortinet®E, FortiGate®E, and FortiGuard®E are registered trademarks of Fortinet, Inc., and other Fortinet names may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2018 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.

Product License Agreement

The parties to this agreement are you, the end customer, and either (i) where you have purchased your Product within the Americas, Fortinet, Inc., or (ii) where you

☒ I accept all license agreements.

CANCEL

BACK

NEXT

9. In **6 Select Storage** select the following, then click **Next**:

- A disk format from the **Select virtual disk format** drop-down list. Select **Thin Provision**.
- A **VM Storage Policy** from the drop-down list.
- Select **Disable Storage DRS for this virtual machine**, if necessary, and choose the storage DRS from the table.

FortiSIEM 6.1.1 ESX Installation and Migration Guide
Fortinet Inc.

9

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- 6 Select storage**
- 7 Select networks
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

Select virtual disk format: Thin Provision

VM Storage Policy:

☐ Disable Storage DRS for this virtual machine

Name	Capacity	Provisioned	Free	Type
NPL_DSCluster	100.04 TB	58.07 TB	41.97 TB	
_templates	931.25 GB	133.79 GB	918.01 GB	VM
archive	2.73 TB	1.14 TB	1.59 TB	VM
ISO	931.25 GB	67.6 GB	863.65 GB	VM

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

10. In **7 Select networks**, select the source and destination networks from the drop down lists. Click **Next**.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- 7 Select networks**
- 8 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
NAT	VLAN- Sanbox

1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

11. In **8 Ready to complete**, review the information and click **Finish**.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

✓ 5 License agreements

✓ 6 Select storage

✓ 7 Select networks

8 Ready to complete

Ready to complete

Click Finish to start creation.

Provisioning type	Deploy OVF From Remote URL
Name	FortiSIEM-VA-6.1.1.0118
Template name	FortiSIEM-VA-6.1.1.0118
Download size	3.8 GB
Size on disk	5.7 GB
Folder	US-NPL
Resource	NPL
Storage mapping	1
All disks	Datastore: NPL_DScluster; Format: Thin provision
Network mapping	1
NAT	VLAN220-172.30.56.0_22 - Sanbox
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

CANCEL

BACK

FINISH

12. In the VSphere client, go to your installed OVA.
13. Right-click your installed OVA (example: `FortiSIEM-611.0118.ova`) and select **Edit Settings > VM Options > General Options**. Setup **Guest OS** and **Guest OS Version** (Linux and 64-bit).
14. Open the **Virtual Hardware** tab. Set **CPU** to 16 and **Memory** to 64GB.
15. Click **Add New Device** and create a device.

Add additional disks to the virtual machine definition. These will be used for the additional partitions in the virtual appliance. An All In One deployment requires the following additional partitions.

Disk	Size	Disk Name
Hard Disk 2	100GB	/opt For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when <code>configFSM.sh</code> runs.

Disk	Size	Disk Name
Hard Disk 3	60GB	/cmdb
Hard Disk 4	60GB	/svn
Hard Disk 5	60GB+	/data (see the following note)

Note on Hard Disk 5:

- Add a 5th disk if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.
- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the [FortiSIEM Sizing Guide](#) for additional information.
- NFS or Elasticsearch event DB storage is mandatory for multi-node cluster deployments.

Edit Settings
1-Super-6.1.1.0118-5729-oct26

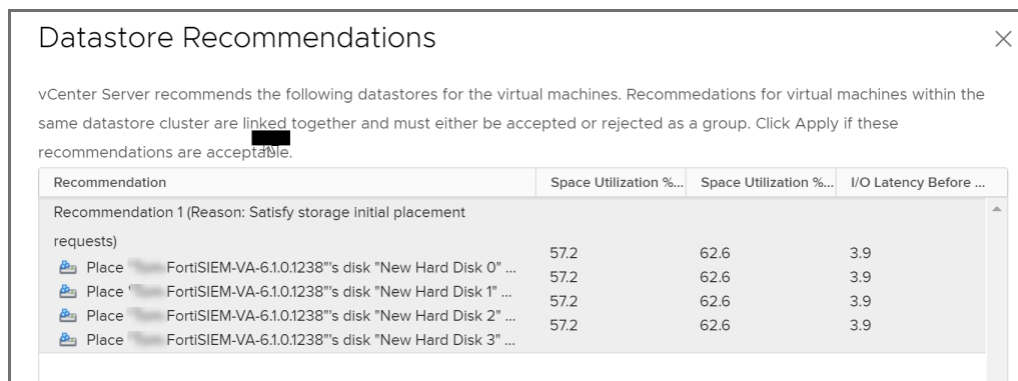
Virtual Hardware
VM Options

ADD NEW DEVICE

> CPU	8		
> Memory	24	GB	
> Hard disk 1	25	GB	
> Hard disk 2	100	GB	
> Hard disk 3	60	GB	
> Hard disk 4	60	GB	
> SCSI controller 0	VMware Paravirtual		
> Network adapter 1	VLAN220-172.30.56.0_22 - Si		<input checked="" type="checkbox"/> Connected
> Video card	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
> Other	Additional Hardware		

CANCEL
OK

After you click **OK**, a Datastore Recommendations dialog box opens. Click **Apply**.



16. Do not turn off or reboot the system during deployment, which may take 7 to 10 minutes to complete. When the deployment completes, click **Close**.

Edit FortiSIEM Hardware Settings

1. In the VMware vSphere client, select the imported Supervisor.
2. Go to **Edit Settings > Virtual hardware**.
3. Set hardware settings as in [Pre-Installation Checklist](#). The recommended settings for the Supervisor node are:
 - CPU = 16
 - Memory = 64 GB
 - Four hard disks:
 - OS – 25GB
 - OPT – 100GB
 - CMDB – 60GB
 - SVN – 60GB

Example settings for the Supervisor node:

Edit Settings
1-Super-6.1.1.0118-5729-oct26

Virtual Hardware
VM Options

ADD NEW DEVICE

> CPU	8		
> Memory	24	GB	
> Hard disk 1	25	GB	
> Hard disk 2	100	GB	
> Hard disk 3	60	GB	
> Hard disk 4	60	GB	
> SCSI controller 0	VMware Paravirtual		
> Network adapter 1	VLAN220-172.30.56.0_22 - Si		<input checked="" type="checkbox"/> Connected
> Video card	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
> Other	Additional Hardware		

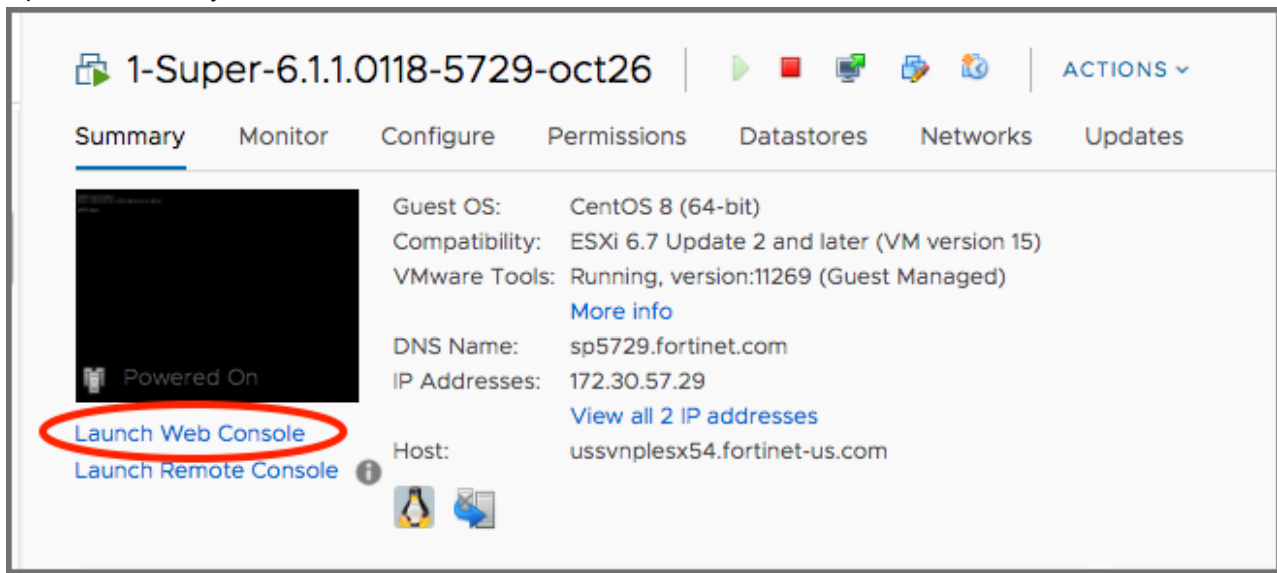
CANCEL
OK

- If event database is local, then choose another disk for storing event data based on your needs.
- Network Interface card

Start FortiSIEM from the VMware Console

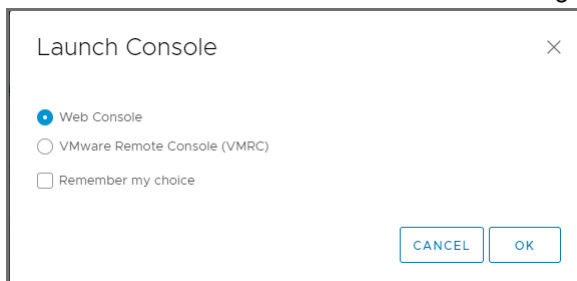
1. In the VMware vSphere client, select the Supervisor, Worker, or Collector virtual appliance.
2. Right-click to open the options menu and select **Power > Power On**.

- Open the Summary tab for the , select **Launch Web Console**.



Network Failure Message: When the console starts up for the first time you may see a Network eth0 Failed message, but this is expected behavior.

- Select **Web Console** in the Launch Console dialog box.



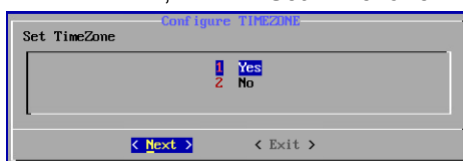
- When the command prompt window opens, log in with the default login credentials – user: `root` and Password: `ProspectHills`.
- You will be required to change the password. Remember this password for future use.

At this point, you can continue configuring FortiSIEM by [using the GUI](#).

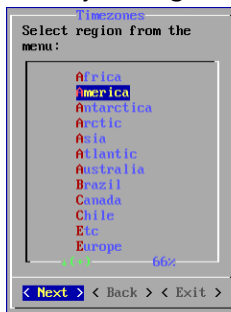
Configure FortiSIEM via GUI

Follow these steps to configure FortiSIEM by using a simple GUI.

- Log in as user `root` with the password you set in [Step 6](#) above.
- At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`configFSM.sh`
- In VM console, select **1 Set Timezone** and then press **Next**.



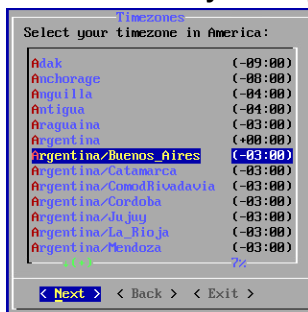
4. Select your **Region**, and press **Next**.



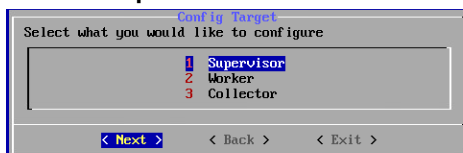
5. Select your **Country**, and press **Next**.



6. Select the **Country** and **City** for your timezone, and press **Next**.

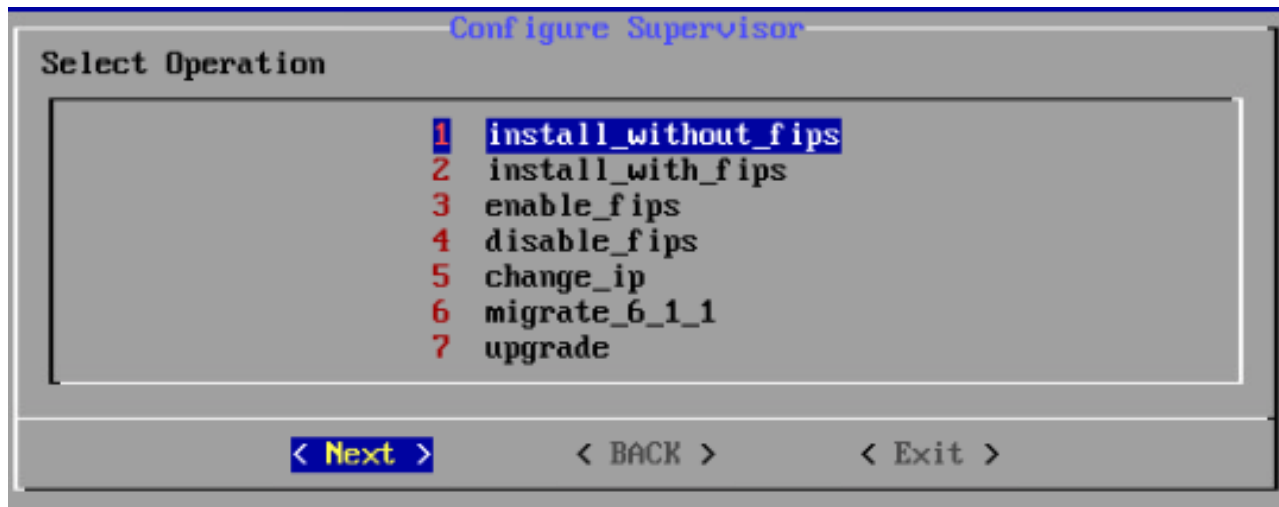


7. Select **1 Supervisor**. Press **Next**.



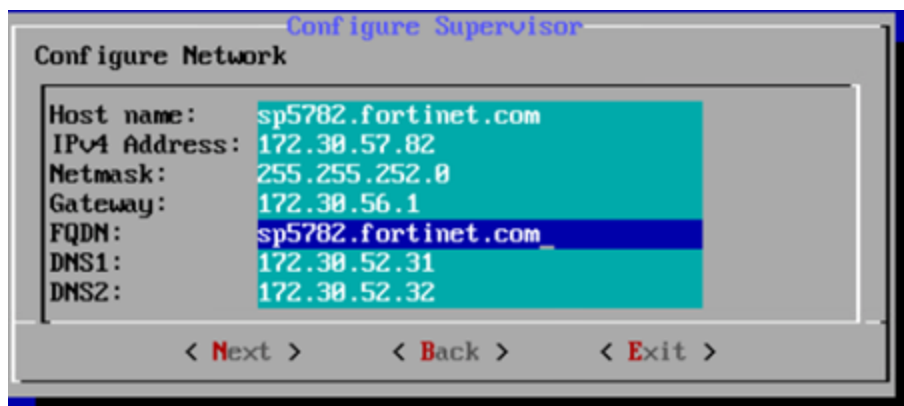
Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

8. If you want to enable FIPS, then choose **2**. Otherwise, choose **1**. You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.



9. Configure the network by entering the following fields. Press **Next**.

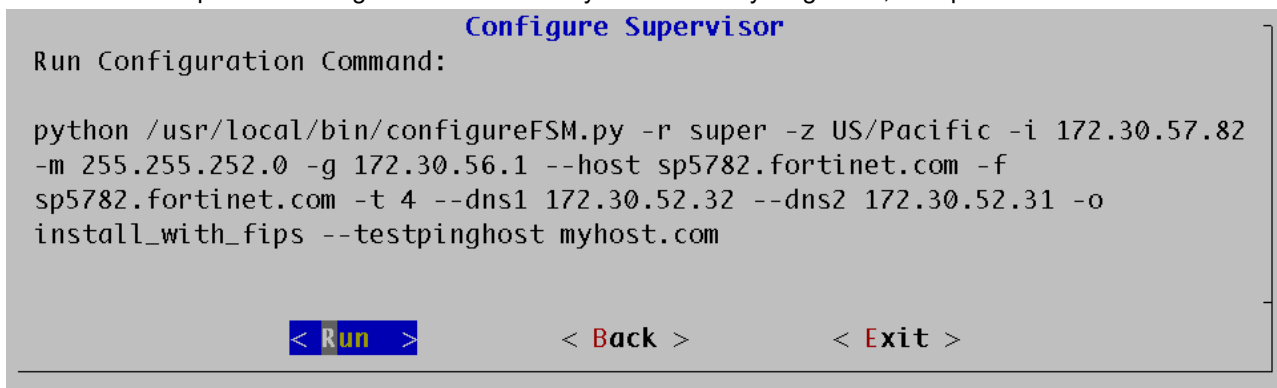
Option	Description
Host Name	The Supervisor's host name
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS server 1 and DNS server2



10. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.



11. The final configuration confirmation is displayed. Verify that the parameters are correct. If they are not, then press **Back** to return to previous dialog boxes to correct any errors. If everything is OK, then press **Run**.



The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
--host	Host name
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either 4 (for ipv4) or 6 (for v6) Note: the 6 value is not currently supported.
--dns1, --dns2	Addresses of DNS server 1 and DNS server 2.
-o	Installation option (install_without_fips , install_with_fips , enable_fips , disable_fips , or change_ip)
-Z	Time zone. Possible values are US/Pacific , Asia/Shanghai , Europe/London , or

Option	Description
Africa/Tunis	
--testpinghost	The URL used to test connectivity

- It will take some time for this process to finish. When it is done, proceed to [Upload the FortiSIEM License](#). If the VM fails, you can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` to try and identify the problem.

Upload the FortiSIEM License



Before proceeding, make sure that you have obtained valid FortiSIEM license from Forticare. For more information, see the [Licensing Guide](#).

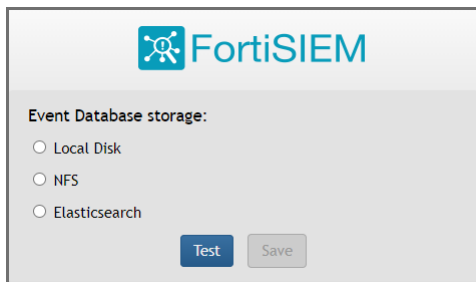
You will now be asked to input a license.

- Open a Web browser and log in to the FortiSIEM UI.
- The License Upload dialog box will open.

- Click **Browse** and upload the license file.
Make sure that the **Hardware ID** shown in the License Upload page matches the license.
- For **User ID** and **Password**, choose any **Full Admin** credentials.
For the first time installation, enter `admin` as the user and `admin*1` as the password. You will then be asked to create a new password for GUI access.
- Choose **License type** as **Enterprise** or **Service Provider**.
This option is available only for a first time installation. Once the database is configured, this option will not be available.
- Proceed to [Choose an Event Database](#).

Choose an Event Database

For a fresh installation, you will be taken to the Event Database Storage page. You will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options. For more details, see [Configuring Storage](#).



After the License has been uploaded, and the Event Database Storage setup is configured, FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

You can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` if you encounter any issues during FortiSIEM installation.

After installation completes, ensure that the `phMonitor` is up and running, for example:

```
# phstatus
```

The response should be similar to the following.

```
Every 1.0s: /opt/phoenix/bin/phstatus.py
System uptime: 21:12:02 up 1:11, 1 user, load average: 0.16, 0.20, 0.36
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16.0% user, 6.2% sys, 0.0% id, 91.4% idle, 0.0% wa, 0.2% hi, 0.1% si, 0.0% st
Mem: 65782100k total, 18366836k used, 55336864k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465828k cached

PROCESS                UPTIME                CPU%                VIRT_MEM            RES_MEM
phParser                41:23                0                    2176m                550m
phQueryMaster           41:41                0                    1820m                77m
phRuleMaster            41:41                0                    1972m                594m
phRuleWorker            41:41                0                    1363m                295m
phQueryWorker           41:41                0                    1383m                279m
phDataManager           41:41                0                    1419m                285m
phDiscover              41:41                0                    513m                 53m
phReportWorker          41:41                0                    1433m                95m
phReportMaster          41:41                0                    683m                 67m
phIdentityWorker        41:41                0                    1827m                50m
phIdentityMaster        41:41                0                    491m                 39m
phAgentManager          41:41                0                    1425m                54m
phCheckpoint            42:31                0                    325m                 34m
phPerfMonitor           41:41                0                    782m                 70m
phReportLoader          41:41                0                    769m                270m
phBeaconEventPackager   41:41                0                    1125m                65m
phDataPurger            41:41                0                    580m                 50m
phEventForwarder        41:41                0                    540m                 46m
phMonitor               37:24                0                    2880m                53m
Apache                  01:10:40             0                    310m                 16m
Node.js-charting        01:10:19             0                    916m                 71m
Node.js-pm2             01:10:13             0                    26m                  26m
AppSvc                  01:10:07             0                    15172m               3826m
DBSvc                   01:10:30             0                    317m                 30m
phAnomaly               01:00:07             0                    907m                 64m
phFortiInsightAI        01:10:40             0                    23432m               430m
Redis                   01:10:10             0                    55m                  25m
```

Cluster Installation

For larger installations, you can choose Worker nodes, Collector nodes, and external storage (NFS or Elasticsearch).

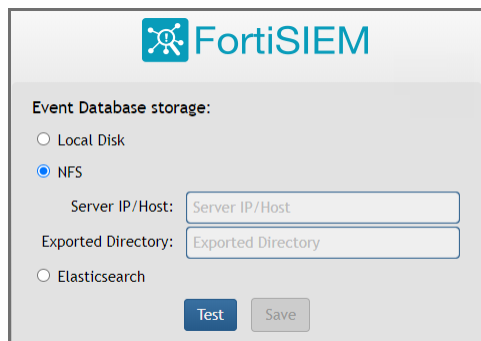
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Install Collectors](#)
- [Register Collectors](#)

Install Supervisor

Follow the steps in [All-in-one Install](#) with two differences:

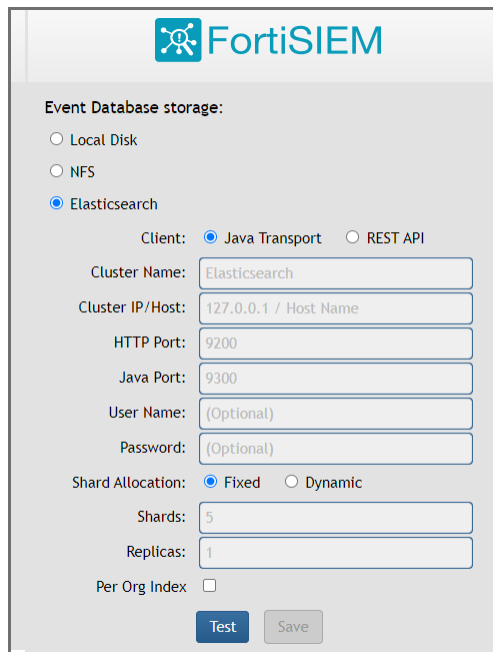
- Setting up hardware - you do not need an event database.
- Setting up an external Event database - configure the cluster for either NFS or Elasticsearch.

NFS



The screenshot shows the FortiSIEM configuration interface for NFS storage. At the top is the FortiSIEM logo. Below it, the section 'Event Database storage:' contains three radio buttons: 'Local Disk', 'NFS' (which is selected), and 'Elasticsearch'. Under the 'NFS' option, there are two text input fields: 'Server IP/Host' with the placeholder text 'Server IP/Host' and 'Exported Directory' with the placeholder text 'Exported Directory'. At the bottom of the form are two buttons: 'Test' and 'Save'.

Elasticsearch



The screenshot shows the FortiSIEM configuration interface for Elasticsearch storage. At the top is the FortiSIEM logo. Below it, the section 'Event Database storage:' contains three radio buttons: 'Local Disk', 'NFS', and 'Elasticsearch' (which is selected). Under the 'Elasticsearch' option, there is a 'Client:' section with two radio buttons: 'Java Transport' (selected) and 'REST API'. Below this are several text input fields: 'Cluster Name' with the placeholder 'Elasticsearch', 'Cluster IP/Host' with the placeholder '127.0.0.1 / Host Name', 'HTTP Port' with the placeholder '9200', 'Java Port' with the placeholder '9300', 'User Name' with the placeholder '(Optional)', and 'Password' with the placeholder '(Optional)'. There is also a 'Shard Allocation:' section with two radio buttons: 'Fixed' (selected) and 'Dynamic'. Below this are two more text input fields: 'Shards' with the placeholder '5' and 'Replicas' with the placeholder '1'. At the bottom, there is a 'Per Org Index' checkbox which is unchecked. At the very bottom are two buttons: 'Test' and 'Save'.

You must choose external storage listed in [Choose an Event Database](#).

Install Workers

Once the Supervisor is installed, follow the same steps in [All-in-one Install](#) to install a Worker except only choose OS and OPT disks. The recommended CPU and memory settings for Worker node, and required hard disk settings are:

- CPU = 8
- Memory = 24 GB
- Two hard disks:
 - OS – 25GB

- OPT – 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Edit Settings
1-Worker-6.1.1.0118-57108-oct26

Virtual Hardware
VM Options

ADD NEW DEVICE

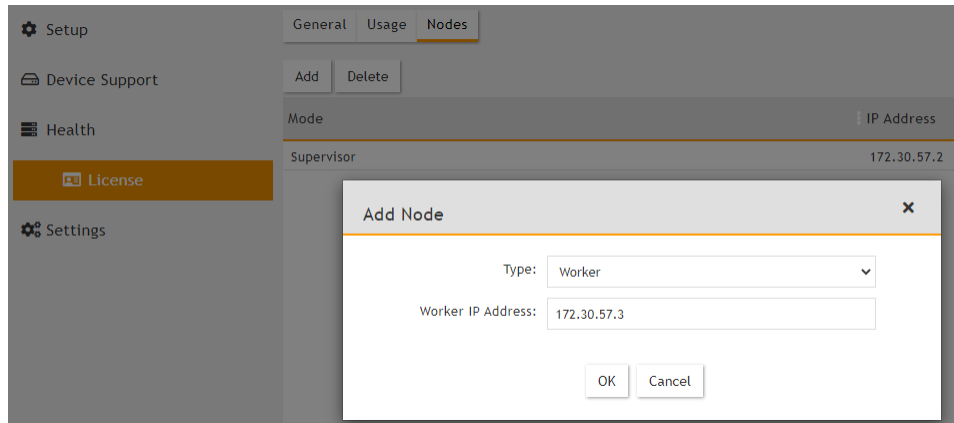
> CPU	8	▼	
> Memory	24	GB	▼
> Hard disk 1	25	GB	▼
> Hard disk 2	100	GB	▼
> SCSI controller 0	VMware Paravirtual		
> Network adapter 1	VLAN220-172.30.56.0_22 - Si		<input checked="" type="checkbox"/> Connected
> Video card	Specify custom settings ▼		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
> Other	Additional Hardware		

CANCEL
OK

Register Workers

Once the Worker is up and running, add the Worker to the Supervisor node.

1. Go to **ADMIN > License > Nodes**.
2. Select **Worker** from the drop-down list and enter the Worker's IP address. Click **Add**.



3. See **ADMIN > Health > Cloud Health** to ensure that the Workers are up, healthy, and properly added to the system.

Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used
sp572.fortinet.com	172.30.57.2	Supervisor	Normal	6.1.0.1238	0.95,0.47,0.43	4%	0 KB
wk573.fortinet.com	172.30.57.3	Worker	Normal	6.1.0.1238	0.1,0.2,0.16	2%	0 KB

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
Node.js-charting	Up	1h 3m	0%	70 MB	916 MB		
httpd	Up	14m 6s	0%	16 MB	310 MB		
Redis	Up	14m 6s	0%	22 MB	51 MB		
Node.js-pm2	Up	1h 3m	0%	44 MB	899 MB		
rsyslogd	Up	1h 3m	0%	7 MB	189 MB		
phDataManager	Up	14m 6s	0%	103 MB	1229 MB	1	126108

Install Collectors

Once Supervisor and Workers are installed, follow the same steps in [All-in-one Install](#) to install a Collector except in [Edit FortiSIEM Hardware Settings](#), only choose OS and OPT disks. The recommended CPU and memory settings for Collector node, and required hard disk settings are:

- CPU = 4
- Memory = 8GB
- Two hard disks:
 - OS – 25GB
 - OPT – 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- [Enterprise Deployments](#)
- [Service Provider Deployments](#)

Enterprise Deployments

For Enterprise deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
 - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
 - Note:** Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
 - b. Click **OK**.
3. Go to **ADMIN > Setup > Collectors** and add a Collector by entering:
 - a. **Name** – Collector Name
 - b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
 - c. **Start Time** and **End Time** – set to **Unlimited**.
4. SSH to the Collector and run following script to register Collectors:


```
# /opt/phoenix/bin/phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization> <CollectorName>
```

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

 - a. Set `user` and `password` using the admin user name and password for the Supervisor.
 - b. Set `Super IP or Host` as the Supervisor's IP address.
 - c. Set `Organization`. For Enterprise deployments, the default name is Super.
 - d. Set `CollectorName` from [Step 2a](#).

The Collector will reboot during the Registration.
5. Go to **ADMIN > Health > Collector Health** for the status.

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	1.1.1.1	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

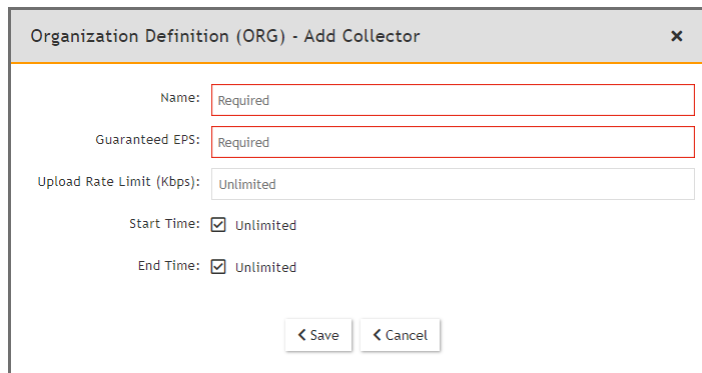
Service Provider Deployments

For Service Provider deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
 - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
 - b. Click **OK**.

3. Go to **ADMIN > Setup > Organizations** and click **New** to add an Organization.

4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
5. Under **Collectors**, click **New**.
6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.
 The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.



Organization Definition (ORG) - Add Collector

Name: Required

Guaranteed EPS: Required

Upload Rate Limit (Kbps): Unlimited

Start Time: ☒ Unlimited

End Time: ☒ Unlimited

< Save < Cancel

7. SSH to the Collector and run following script to register Collectors:

```
# /opt/phoenix/bin/phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization> <CollectorName>
```

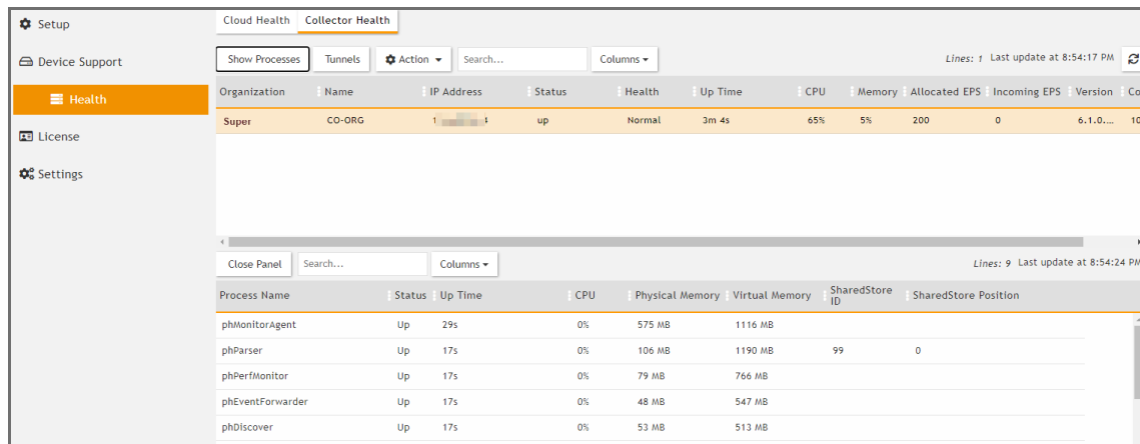
The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- Set user and password using the admin user name and password for the Organization that the Collector is going to be registered to.
- Set Super IP or Host as the Supervisor's IP address.
- Set Organization as the name of an organization created on the Supervisor.
- Set CollectorName from [Step 6](#).

```
root@co574 ~# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
root@co574 ~# phProvisionCollector --add admin Admin=11 172.30.57.2 ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
root@co574 ~# _
```

The Collector will reboot during the Registration.

8. Go to **ADMIN > Health > Collector Health** and check the status.



The screenshot shows the 'Collector Health' page in the FortiSIEM interface. It displays a table of collector status and a detailed view of the 'phMonitorAgent' process.

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	172.30.57.2	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

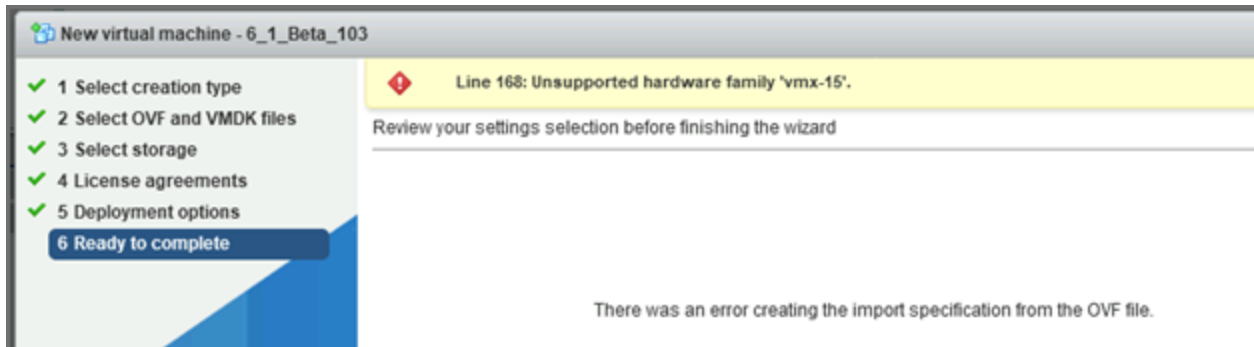
Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Installing on ESX 6.5

- [Importing a 6.5 ESX Image](#)
- [Resolving Disk Save Error](#)
- [Adding a 5th Disk for /data](#)

Importing a 6.5 ESX Image

When installing with ESX 6.5, or an earlier version, you will get an error message when you attempt to import the image.



To resolve this import issue, you will need to take the following steps:

1. Install 7-Zip.
2. Extract the OVA file into a directory.
3. In the directory where you extracted the OVA file, edit the file `FortiSIEM-VA-6.1.1.0118.ovf`, and replace all references to `vmx-15` with your compatible ESX hardware version shown in the following table.

Note: For example, for ESX 6.5, replace `vmx-15` with `vmx-13`.

```
<?xml version='1.0' encoding='UTF-8'>
<VirtualHardwareSection>
  <Info>Virtual hardware requirements for a virtual machine</Info>
  <System>
    <vssd:ElementName>Virtual Hardware Family</vssd:ElementName>
    <vssd:InstanceID>0</vssd:InstanceID>
    <vssd:VirtualSystemIdentifier>FSM-VA-C8</vssd:VirtualSystemIdentifier>
    <vssd:VirtualSystemType>vmx-15</vssd:VirtualSystemType>
  </System>
  <Item>
    <rasd:Caption>4 virtual CPU</rasd:Caption>
    <rasd:Description>Number of virtual CPUs</rasd:Description>
    <rasd:ElementName>16 virtual CPU</rasd:ElementName>
```

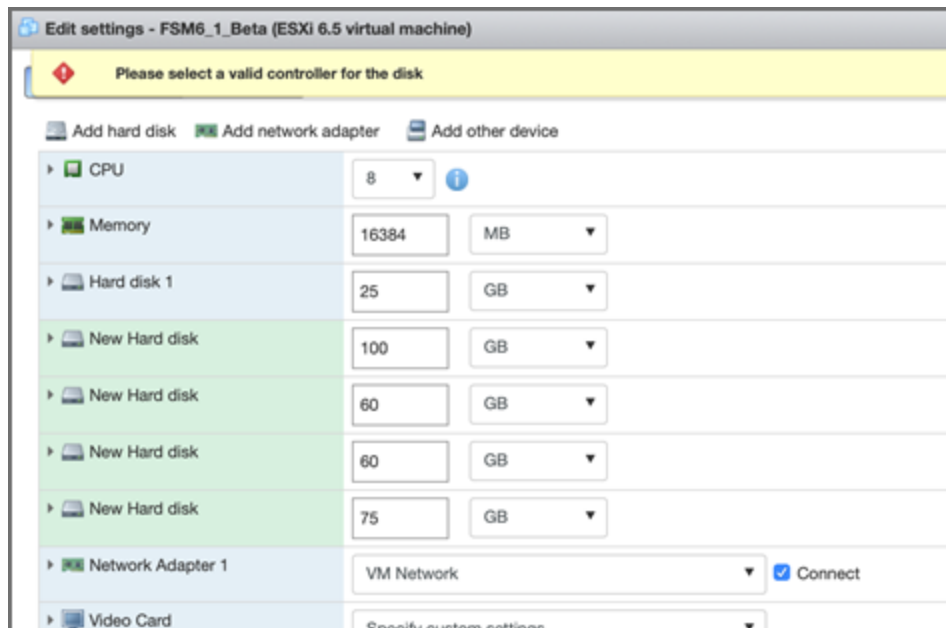
Compatibility	Description
ESXi 6.5 and later	This virtual machine (hardware version 13) is compatible with ESXi 6.5.
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0 and ESXi 6.5.

Compatibility	Description
ESXi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5, ESXi 6.0, and ESXi 6.5.
ESXi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
ESXi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
ESX/ESXi 4.0 and later	This virtual machine (hardware version 7) is compatible with ESX/ESXi 4.0, ESX/ESXi 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
ESX/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESXi 3.5, ESX/ESXi 4.0, ESX/ESXi 4.1, ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5. It is also compatible with VMware Server 1.0 and later. ESXi 5.0 does not allow creation of virtual machines with ESX/ESXi 3.5 and later compatibility, but you can run such virtual machines if they were created on a host with different compatibility.
ESX Server 2.x and later	This virtual machine (hardware version 3) is compatible with ESX Server 2.x, ESX/ESXi 3.5, ESX/ESXi 4.0, ESX/ESXi 4.1, and ESXi 5.0. You cannot create, edit, turn on, clone, or migrate virtual machines with ESX Server 2.x compatibility. You can only register or upgrade them.

Note: For more information, see [here](#).

Resolving Disk Save Error

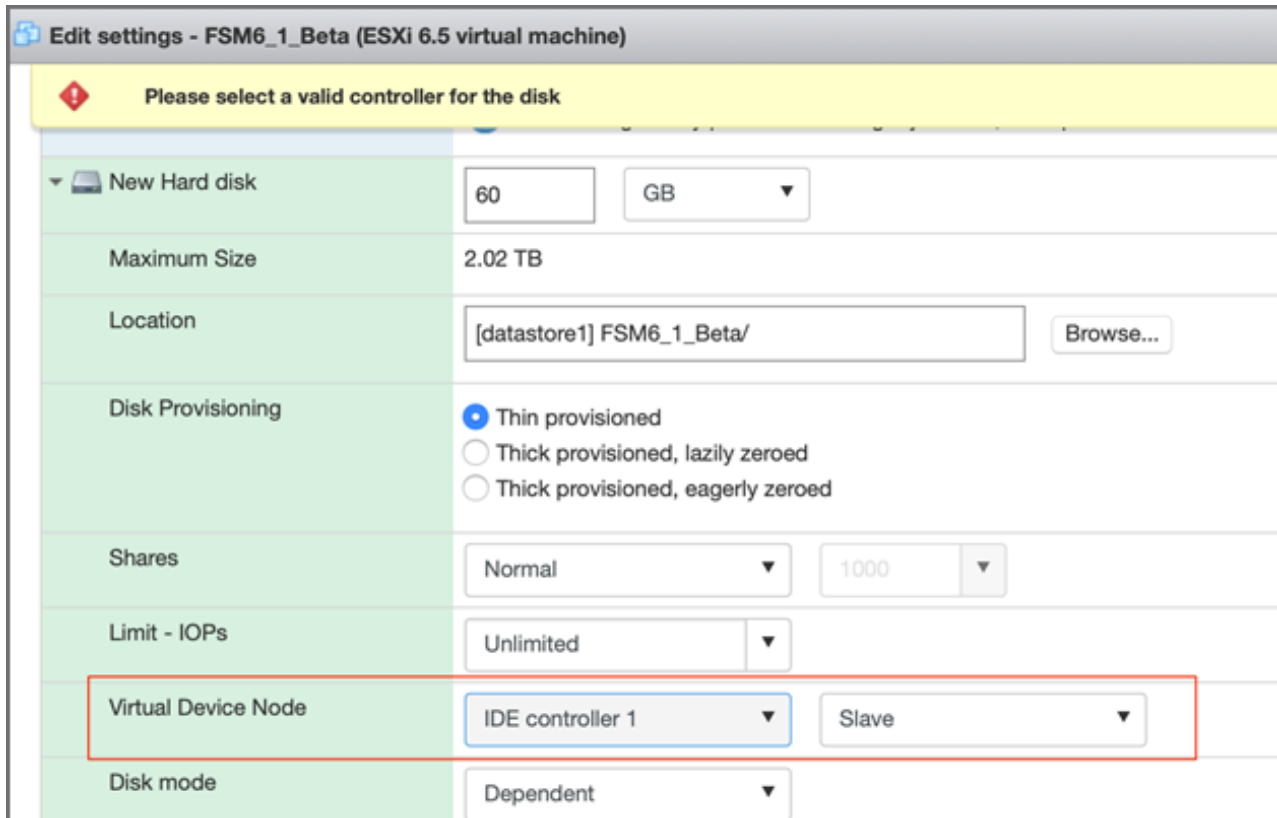
You may encounter an error message asking you to select a valid controller for the disk if you attempt to add an additional 4th disk (`/opt`, `/cmd`, `/svn`, and `/data`). This is likely due to an old IDE controller issue in VMware, where you are normally limited to 2 IDE controllers, 0, 1, and 2 disks per controller (Master/Slave).



If you are attempting to add 5 disks in total, such as this following example, you will need to take the following steps:

Disk	Usage
1st	25GB default for image
2nd	100GB for /opt For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when <code>configFSM.sh</code> runs.
3rd	60GB for /cndb
4th	60GB for /svn
5th	75GB for /data (optional, or use with NFS or ES storage)

1. Go to Edit settings, and add each disk individually, clicking save after adding each disk.
When you reach the 4th disk, you will receive the "Please select a valid controller for the disk" message. This is because the software has failed to identify the virtual device node controller/Master or Slave for some unknown reason.
2. Expand the disk setting for each disk and review which IDE Controller Master/Slave slots are in use. For example, in one installation, there may be an attempt for the 4th disk to be added to IDE Controller 0 when the Master/Slave slots are already in use. In this situation, you would need to put the 4th disk on IDE Controller 1 in the Slave position, as shown here. In your situation, make the appropriate configuration setting change.



Edit settings - FSM6_1_Beta (ESXi 6.5 virtual machine)

Please select a valid controller for the disk

New Hard disk	60	GB
Maximum Size	2.02 TB	
Location	[datastore1] FSM6_1_Beta/ Browse...	
Disk Provisioning	<input checked="" type="radio"/> Thin provisioned <input type="radio"/> Thick provisioned, lazily zeroed <input type="radio"/> Thick provisioned, eagerly zeroed	
Shares	Normal	1000
Limit - IOPs	Unlimited	
Virtual Device Node	IDE controller 1	Slave
Disk mode	Dependent	

3. Click save to ensure your work has been saved.

Adding a 5th Disk for /data

When you need to add a 5th disk, such as for `/data`, and there is no available slot, you will need to add a SATA controller to the VM by taking the following steps:

1. Go to Edit settings.
2. Select **Add Other Device**, and select **SCSI Controller** (or SATA).

You will now be able to add a 5th disk for `/data`, and it should default to using the additional controller. You should be able to save and power on your VM. At this point, follow the normal instructions for installation.

Note: When adding the local disk in the GUI, the path should be `/dev/sda` or `/dev/sdd`. You can use one of the following commands to locate:

```
# fdisk-l
or
# lsblk
```

Migrating from FortiSIEM 5.3.x or 5.4.0

Migration limitations: If migrating from 5.3.3 or 5.4.0 to 6.1.1, please be aware that the following features will not be available after migration.

- Pre-compute feature
- Elastic Cloud support

If any of these features are critical to your organization, then please wait for a later version where these features are available after migration.

This section describes how upgrade from FortiSIEM 5.3.x or 5.4.0 to FortiSIEM 6.1.1. FortiSIEM performs migration in-place, via a bootloader. There is no need to create a new image or copy disks. The bootloader shell contains the new version of FortiSIEM.

- [Pre-Migration Checklist](#)
- [Migrate All-in-one Installation](#)
- [Migrate Cluster Installation](#)

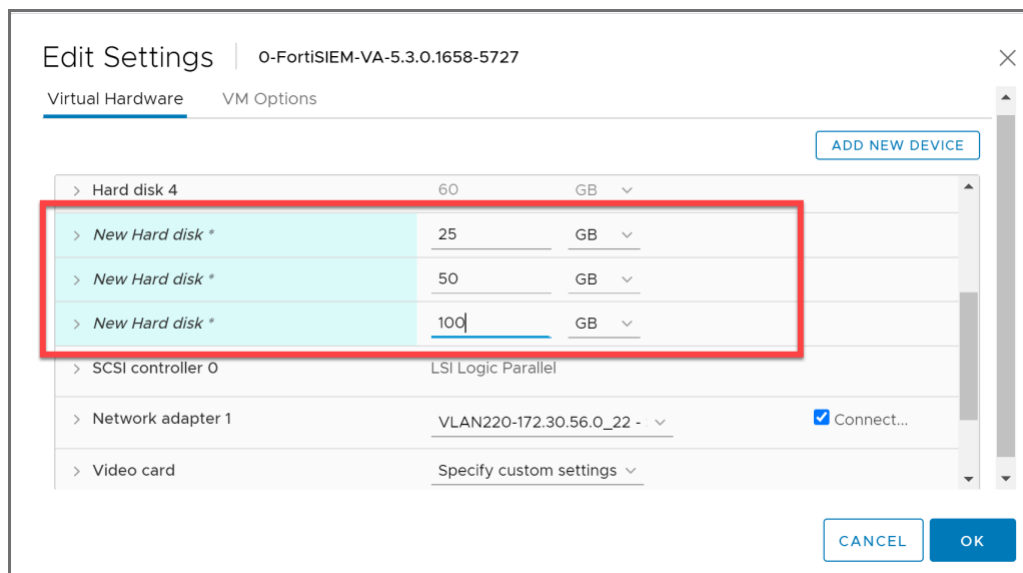
Pre-Migration Checklist

To perform the migration, the following prerequisites must be met

1. Release 6.1.1 requires at least ESX 6.5, and ESX 6.7 Update 2 is recommended.
2. Ensure that your system can connect to the network. You will be asked to provide a DNS Server and a host that can be resolved by the DNS Server and can respond to a ping. The host can either be an internal host or a public domain host like google.com.
3. Make sure you are running 5.3.x or 5.4.0, since 6.1.1 migration is only supported from these versions. If you are running a version earlier than 5.3.0, then upgrade to any of these versions first (recommended 5.4.0) and then follow the procedures below.
4. Take a SnapShot of the running FortiSIEM instance.
5. Delete Worker from Super GUI.
6. Stop/Shutdown the Worker.
7. Make sure the `root` directory (/) has at least 1 GB of available space.
8. Right click the FortiSIEM OVA in VCenter and choose **Edit Settings**.
9. In the VM Hardware tab, click **Add New Device > Hard Disk** to add a disk with 25GB of space. Repeat this process to add disks with 50GB and 100GB of space. There should be a total of 7 disks: 4 existing disks using local storage and the 3 disks you just added. Click **OK** when you are finished.



You can find detailed information about installing FortiSIEM and configuring disks in [Fresh Installation](#).



10. Review the list of Datastores and click **Apply**.
11. In VCenter, right click the FortiSIEM VM and select **Power On**.
12. In the VCenter Summary tab, click **Launch Web Console**.
13. Log in to the console as user `root`, with password `ProspectHills`.
14. In the console, run `fdisk -l`, for example:
`fdisk -l`



Note the list of the partition tables, the disk names, their approximate sizes and the UUID value. You will need this information for a later step.


```

Disk identifier: 0x000ac8e6

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1            1         7832     62910539+   83   Linux

Disk /dev/sdd: 64.4 GB, 64424509440 bytes
255 heads, 63 sectors/track, 7832 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sdf: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sde: 26.8 GB, 26843545600 bytes
255 heads, 63 sectors/track, 3263 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sdg: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

[root@va5727 ~]# _

```

15. Mount the ~50GB disk to the /images directory. In the console, enter these commands and options:
 - a. Enter `# fdisk /dev/<your_50GB_disk>` Press **Return**.
 - b. Enter `n` to add a new partition. Press **Return**.
 - c. Enter `p` to choose primary partition. Press **Return**.
 - d. Enter `1` to choose partition number. Press **Return**.
 - e. Press **Return** to accept the default.
 - f. Press **Return** to accept the default.
 - g. Enter `w` to write the table to disk and exit. Press **Return**.
 - h. Enter the `mkfs.ext4 /dev/sdf1` command (where `sdf1` is the 50GB disk) to make a file system.
 - i. Enter the `mkdir -p /images` command to create an `images` directory.
 - j. Enter `mount /dev/sdf1 /images` command to mount the 50GB disk to the `/images` directory.
Or using the UUID if the disk name changed, for example:


```
# blkid /dev/sdf1 /dev/sdf1: UUID="d4a5b82f-6e73-456b-ab08-d6e6d845d1aa" TYPE="ext4"
# mount -U d4a5b82f-6e73-456b-ab08-d6e6d845d1aa /images
```
16. Enter the `df -h` command to get the file system disk space usage.
The following screen shot illustrates steps 12 and 13.

```

[root@va57199 /]# fdisk /dev/sdf

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-6657, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-6657, default 6657):
Using default value 6657

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[root@va57199 /]# mkfs.ext4 /dev/sdf1
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
3342336 inodes, 13368080 blocks
668404 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
408 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information:

done

This filesystem will be automatically checked every 36 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
[root@va57199 /]#
[root@va57199 /]#
[root@va57199 /]# mount /dev/sdf1 /images
[root@va57199 /]# df -h

```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda3	55G	36G	17G	69%	/
tmpfs	7.8G	8.0K	7.8G	1%	/dev/shm
/dev/sda1	124M	43M	76M	36%	/boot
/dev/sdb1	60G	453M	56G	1%	/cmdb
/dev/sdc1	60G	181M	56G	1%	/svn
/dev/sdd	79G	210M	75G	1%	/data
/dev/sdf1	51G	52M	48G	1%	/images

```

[root@va57199 /]#

```

17. Copy the `FSM_Full_All_RAW_VM-6.1.1_build0118.zip` file to the `/images` directory. Use `unzip` to extract the 6.1.1 FortiSIEM hardware image.

```
# unzip FSM_Full_All_RAW_VM-6.1.1_build0118.zip
```

Note: The image size is about 25GB after extracting.

18. Create a soft link to the image folder, for example:

```
# ln -sf /images/FortiSIEM-RAW-VM-6.1.1.0118.img /images/latest
```

19. Enter the `ll` command to ensure `latest` link is defined, for example:

```
# ll
```

```
[root@sp5783 images]# ll
total 30049224
-rw-r--r-- 1 root root 26843545600 Oct 26 12:00 FortiSIEM-RAW-VM-6.1.1.0118.img
-rw-r--r-- 1 root root 3926832827 Oct 26 13:19 FSM_Full_All_RAW_VM_6.1.1_build0118.zip
lrwxrwxrwx 1 root root 39 Oct 28 16:28 latest -> /images/FortiSIEM-RAW-VM-6.1.1.0118.img
drwx----- 2 root root 16384 Oct 28 16:23 lost+found
```

Migrate All-in-one Installation

- Download the Bootloader
- Prepare the Bootloader
- Load the FortiSIEM 6.1.1 Image
- Prepare the FortiSIEM VM for 6.1.1
- Migrate to FortiSIEM 6.1.1
- Finishing Up

Download the Bootloader

Install and configure the FortiSIEM bootloader to start migration. Follow these steps:

1. Download the bootloader `FSM_Bootloader_6.1.1_build0118.zip` from the [support site](#) and copy it to the `/images` directory.
2. Unzip the file, for example:

```
# unzip FSM_Bootloader_6.1.1_build0118.zip
```

```
[root@sp5783 images]# ll
total 30325396
-rw-r--r-- 1 root root 26843545600 Oct 26 12:00 FortiSIEM-RAW-VM-6.1.1.0118.img
drwxr-xr-x 2 root root 4096 Oct 28 16:30 FSM_Bootloader_6.1.1_build0118
-rw-r--r-- 1 root root 282794080 Oct 26 13:13 FSM_Bootloader_6.1.1_build0118.zip
-rw-r--r-- 1 root root 3926832827 Oct 26 13:19 FSM_Full_All_RAW_VM_6.1.1_build0118.zip
lrwxrwxrwx 1 root root 39 Oct 28 16:28 latest -> /images/FortiSIEM-RAW-VM-6.1.1.0118.img
drwx----- 2 root root 16384 Oct 28 16:23 lost+found
[root@sp5783 images]# cd FSM_Bootloader_6.1.1_build0118
[root@sp5783 FSM_Bootloader_6.1.1_build0118]# ll
total 276220
-rwxr-xr-x 1 root root 114 Oct 26 10:42 grub.bl.tmpl
-rwxr-xr-x 1 root root 188 Oct 26 10:42 grub.bl.tmpl.hw
-rw-r--r-- 1 root root 277410143 Oct 26 11:23 initramfs.gz
-rw-r--r-- 1 root root 161 Oct 26 10:42 network_params.json
-rw-r--r-- 1 root root 21823 Oct 26 10:42 prepare_bootloader
-rwxr-xr-x 1 root root 50 Oct 26 10:42 pwd_backup
-rwxr-xr-x 1 root root 5392080 Oct 26 11:23 vmlinuz
[root@sp5783 FSM_Bootloader_6.1.1_build0118]#
```

Prepare the Bootloader

Follow these steps to run the `prepare_bootloader` script:

1. Go to the `bootloader` directory, for example:
`# cd /images/FSM_Bootloader_6.1.1_build0118`
2. Run the `prepare_bootloader` script to install and configure the bootloader. This script installs, configures, and reboots the system. The script may take a few minutes to complete.
`# sh prepare_bootloader`
3. The script will open the FortiSIEM bootloader shell.

```
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 34 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').

Command (m for help): Partition number (1-4):
Command (m for help): Command (m for help): Command (m for help): The partition table has been alter
ed!

Calling ioctl() to re-read partition table.

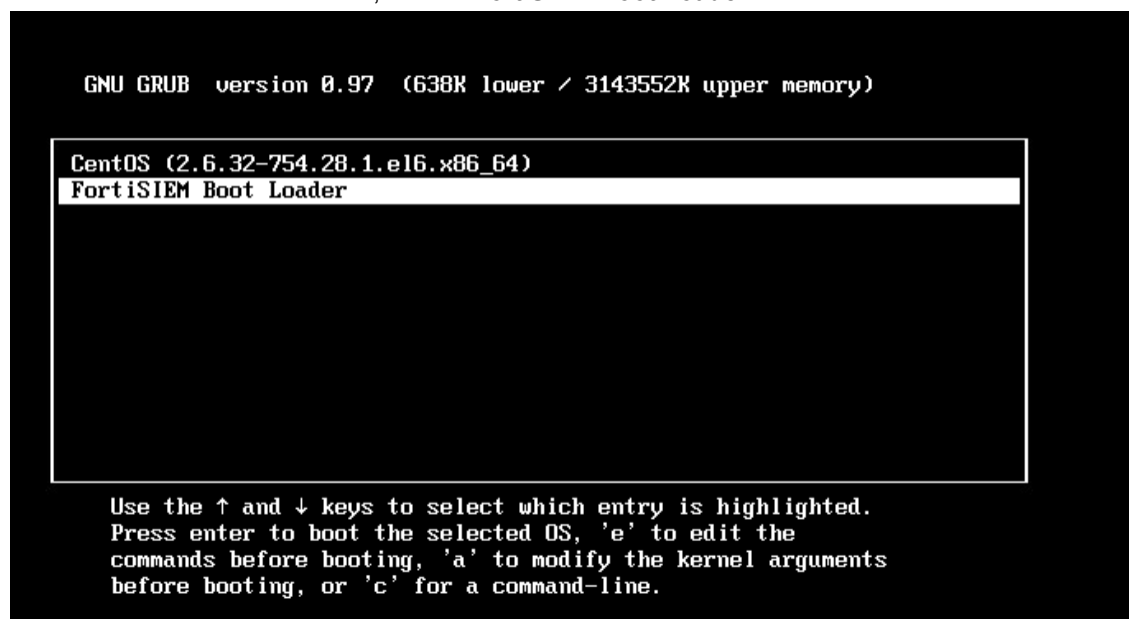
WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script 'grub-install'.

# this device map was generated by anaconda
(hd0)      /dev/sda
(hd4)      /dev/sde
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script 'grub-install'.

# this device map was generated by anaconda
(hd0)      /dev/sda
(hd4)      /dev/sde
Waiting SYSTEM Will be Rebooted
[root@va5727 bootloader]#
```

Note: you might have to reboot the system manually if auto-reboot does not work.

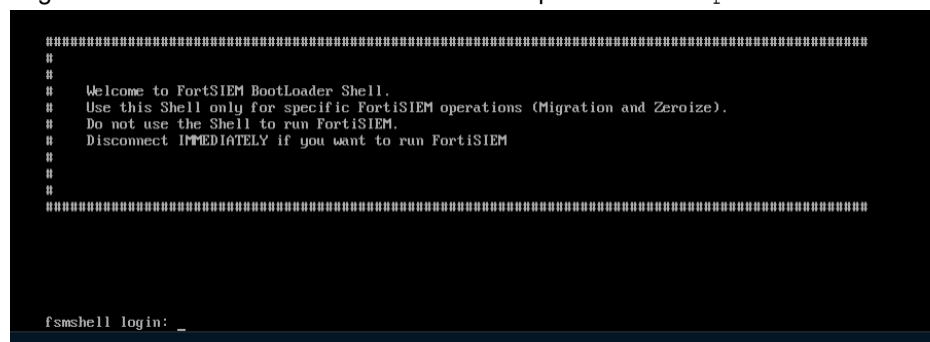
4. In the FortiSIEM bootloader shell, choose **FortiSIEM Boot Loader**. Press Return.



Load the FortiSIEM 6.1.1 Image

Follow these steps to load the FortiSIEM image:

1. Log in to the bootloader shell as user `root` with password `ProspectHills`.



2. Create and mount the `/images` directory:
 - a. Create a `/images` directory if it is not already present, for example:


```
# mkdir -p /images
```
 - b. Mount the `sdf1` (the 50GB disk) to the `/images` directory, for example:


```
# mount /dev/sdf1 /images
```

 Or using the UUID if the disk name changed:


```
# mount -U d4a5b82f-6e73-456b-ab08-d6e6d845d1aa /images
```
 - c. Change to the `/images` directory, for example:


```
# cd /images
```
 - d. Run the `ll` command to check disk usage.


```
# ll
```

These steps are illustrated in the following screen shot.

```
[root@fsmshell images]# ll
total 33647324
-rw-r--r-- 1 root root 9254 Oct 28 19:42 ao_login.png
-rw-r--r-- 1 root root 4739 Oct 28 19:42 ao_upload.png
drwxr-xr-x 6 root root 4096 Oct 28 19:42 backup
-rw-r--r-- 1 root root 938 Oct 28 19:42 bg.png
-rw-r--r-- 1 root root 26843545600 Oct 26 15:00 FortiSIEM-RAW-UM-6.1.1.0118.img
-rw-r--r-- 1 root root 630081428 Oct 28 19:34 fsm_53_glassfish.xz
-rw-r--r-- 1 root root 2771411616 Oct 28 19:41 fsm_53_phoenix.xz
drwxr-xr-x 2 root root 4096 Oct 28 19:43 FSM_Bootloader_6.1.1_build0118
-rw-r--r-- 1 root root 282794080 Oct 26 16:13 FSM_Bootloader_6.1.1_build0118.zip
-rw-r--r-- 1 root root 3926832827 Oct 26 16:19 FSM_Full_All_RAW_UM_6.1.1_build0118.zip
-rw-r--r-- 1 root root 814 Oct 26 22:26 grub_base
lrwxrwxrwx 1 root root 39 Oct 28 19:28 latest -> /images/FortiSIEM-RAW-UM-6.1.1.0118.img
-rw-r--r-- 1 root root 9254 Oct 28 19:42 login.png
drwx----- 2 root root 16384 Oct 28 19:23 lost+found
-rw-r--r-- 1 root root 169 Oct 28 19:42 network_params.json
-rw-r--r-- 1 root root 165 Oct 28 19:42 network_params.json.bak
drwxr-xr-x 2 root root 4096 Oct 28 19:42 org
-rw-r--r-- 1 root root 234 Oct 28 19:42 origdisks
-rw-r--r-- 1 root root 44 Oct 28 19:32 orig_UUID
-rwxr-xr-x 1 root root 20 Jul 8 18:15 passwd
-rw-r--r-- 1 500 501 45675 Oct 26 22:21 phoenix_config.txt
-rwxr-xr-x 1 root root 177 Oct 28 19:32 pwd_backup
-rwxr-xr-x 1 root root 56 Oct 28 19:32 pwd_backup.bak
-rw-r--r-- 1 root root 5602 Oct 28 19:42 upload.png
-rw-rw-r-- 1 500 501 125 Aug 19 18:57 VERSION
-rw-r--r-- 1 root root 3242 Oct 28 19:42 wl_login.png
-rw-r--r-- 1 root root 1114 Oct 28 19:42 wl_upload.png
[root@fsmshell images]# _
```

3. Run the load_image script to swipe the old image with the new image, for example:

a. Change to the root directory and check the contents, for example:

```
# cd /
# ll
[root@fsmshell /]# ll
total 48
lrwxrwxrwx 1 root root 7 Jun 30 15:22 bin -> usr/bin
drwxrwxrwx 4 root root 288 Jun 30 15:23 boot
-rwxr-xr-x 1 root root 3725 Jun 16 03:54 boot_loader_operations.sh
drwxr-xr-x 18 root root 3328 Jun 30 15:22 dev
drwxrwxrwx 76 root root 3708 Jun 30 15:23 etc
drwxr-xr-x 2 root root 40 Nov 5 2016 home
drwxr-xr-x 4 root root 4096 Jun 30 15:18 images
-rwxrwxrwx 1 root root 21368 May 22 01:31 isZero
lrwxrwxrwx 1 root root 7 Jun 30 15:22 lib -> usr/lib
lrwxrwxrwx 1 root root 9 Jun 30 15:22 lib64 -> usr/lib64
-rwxr-xr-x 1 root root 3397 Jun 12 21:32 load_image
drwxr-xr-x 2 root root 40 Nov 5 2016 media
drwxr-xr-x 2 root root 40 Nov 5 2016 mnt
drwxr-xr-x 2 root root 40 Nov 5 2016 opt
dr-xr-xr-x 122 root root 8 Jun 30 15:22 proc
dr-xr-xr-x 3 root root 288 Jun 30 15:22 root
drwxr-xr-x 22 root root 608 Jun 30 15:23 run
lrwxrwxrwx 1 root root 8 Jun 30 15:22/sbin -> usr/sbin
drwxr-xr-x 2 root root 40 Nov 5 2016 srv
dr-xr-xr-x 13 root root 8 Jun 30 15:22 sys
drwxrwxrwt 7 root root 180 Jun 30 16:41 tmp
drwxr-xr-x 13 root root 288 Jun 30 15:22 usr
drwxr-xr-x 19 root root 468 Jun 30 15:22 var
-rwxr-xr-x 1 root root 3927 Jun 9 22:27 zeroize.py
[root@fsmshell /]# sh load_image
Found disk /dev/sde of Required size
Checking Partitions on /dev/sde
sde already has partitions
yes
Running Command: dd if=/images/latest of=/dev/sde bs=512 conv=noerror,sync status=progress
3638109184 bytes (3.6 GB) copied, 148.448543 s, 24.5 MB/s
```

b. Run the load_image script, for example:

```
# sh load_image
```

```
[root@fsmshell /]# sh load_image
Found disk /dev/sde of Required size
Checking Partitions on /dev/sde
sde already has partitions
yes
Running Command: dd if=/images/latest of=/dev/sde bs=512 conv=noerror,sync status=progress
26776572416 bytes (27 GB) copied, 588.843679 s, 45.5 MB/s
52428800+0 records in
52428800+0 records out
26843545600 bytes (27 GB) copied, 596.499 s, 45.0 MB/s
Swiping Image to new disk
[root@fsmshell /]# [ 1174.311179] sde: sde1 sde2
[ 1174.492305] device-mapper: uevent: version 1.0.3
[ 1174.493463] device-mapper: ioctl: 4.34.0-iocli (2015-10-28) initialised: dm-devel@redhat.com
```

When the script completes. Press Return.

- c. Press Return again to end the `load_image` script.
- d. Run the `fdisk -l` command to check that the disks have been configured, for example:

```
# fdisk -l

Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xa9ed2ebc

   Device Boot      Start         End      Blocks    Id System
/dev/sde1 *          2048        2899199       1048576    83  Linux
/dev/sde2            2899200       52428799       25164800    8e  Linux LVM

Disk /dev/sdf: 53.7 GB, 53687091200 bytes, 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xb529cfb3

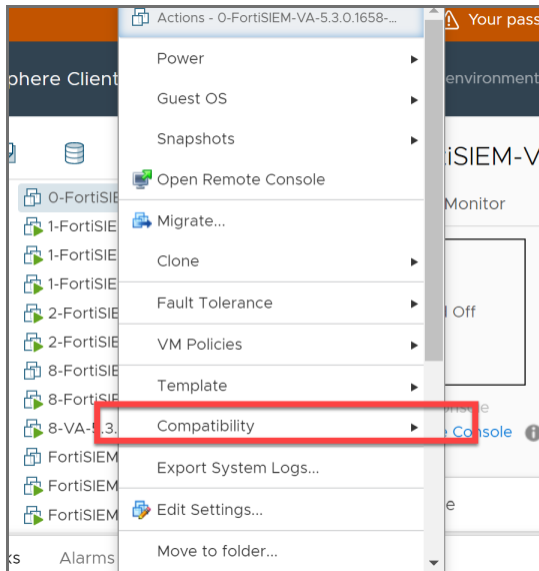
   Device Boot      Start         End      Blocks    Id System
/dev/sdf1            63       104856254       52428096    83  Linux
```

4. In VCenter, power off the VM after `load_image` completes.

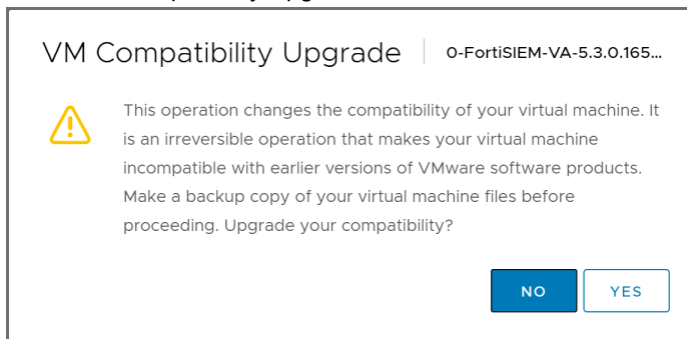
Prepare the FortiSIEM VM for 6.1.1

On the powered off machine from ESXi console, follow these steps to prepare the FortiSIEM VM.

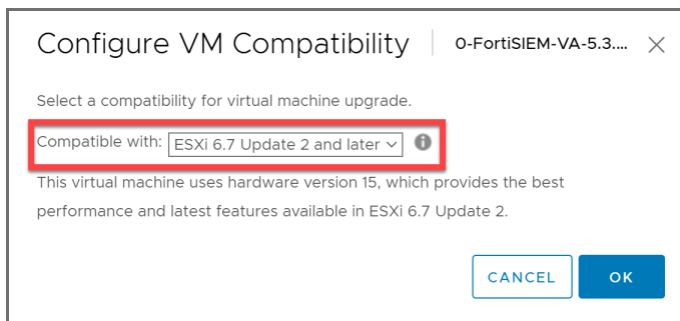
1. In VCenter, right-click the FortiSIEM VM and select **Compatibility > Upgrade VM Compatibility**.



2. In the VM Compatibility Upgrade screen, click **Yes**.



3. In the Configure VM Compatibility screen, select **ESXi 6.7 Update 2 and later** from the **Compatible with:** drop-down list. Click **OK**.



4. Right-click the FortiSIEM VM in VCenter and choose **Edit Settings**.
5. In the Edit Settings dialog box click the **VM Options** tab.
 - a. In **Guest OS**, select **Linux** from the drop-down list.
 - b. In **Guest OS Version**, select **CentOS 8 (64-bit)** from the drop-down list.

c. Click **OK**.

Edit Settings | O-FortiSIEM-VA-5.3.0.1658-5727

Virtual Hardware | **VM Options**

VM Name	O-FortiSIEM-VA-5.3.0.1658-5727
VM Config File	[PVVol_A009] 1-FortiSIEM-VA-5.3.0.1658-5727 FortiSIEM-VA-5.3.0.1658-5727
VM Working Location	[PVVol_A009] 1-FortiSIEM-VA-5.3.0.1658-5727
Guest OS	Linux
Guest OS Version	CentOS 8 (64-bit)
<p>> VMware Remote Console Options</p> <p><input type="checkbox"/> Lock the guest operating system when the last remote user disconnects</p>	

CANCEL OK

6. Open the **Virtual Hardware** tab.

- a. Open the section for the 25GB disk.
- b. Note the SCSI device number of the 25GB disk, for example, SCSI (0 : 4) . You will need this information for a later step.

c. Click **OK**.

Edit Settings

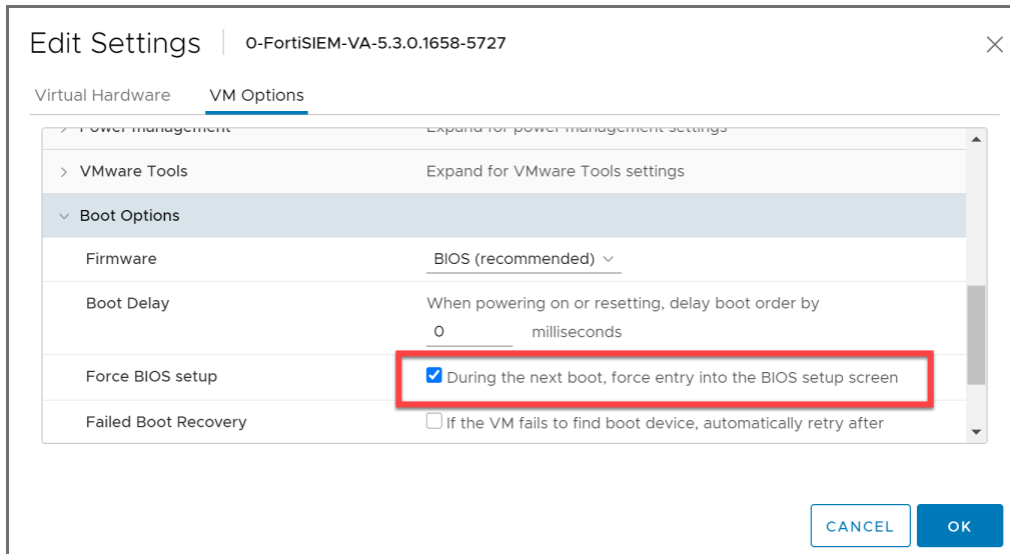
Virtual Hardware
VM Options

ADD NEW DEVICE

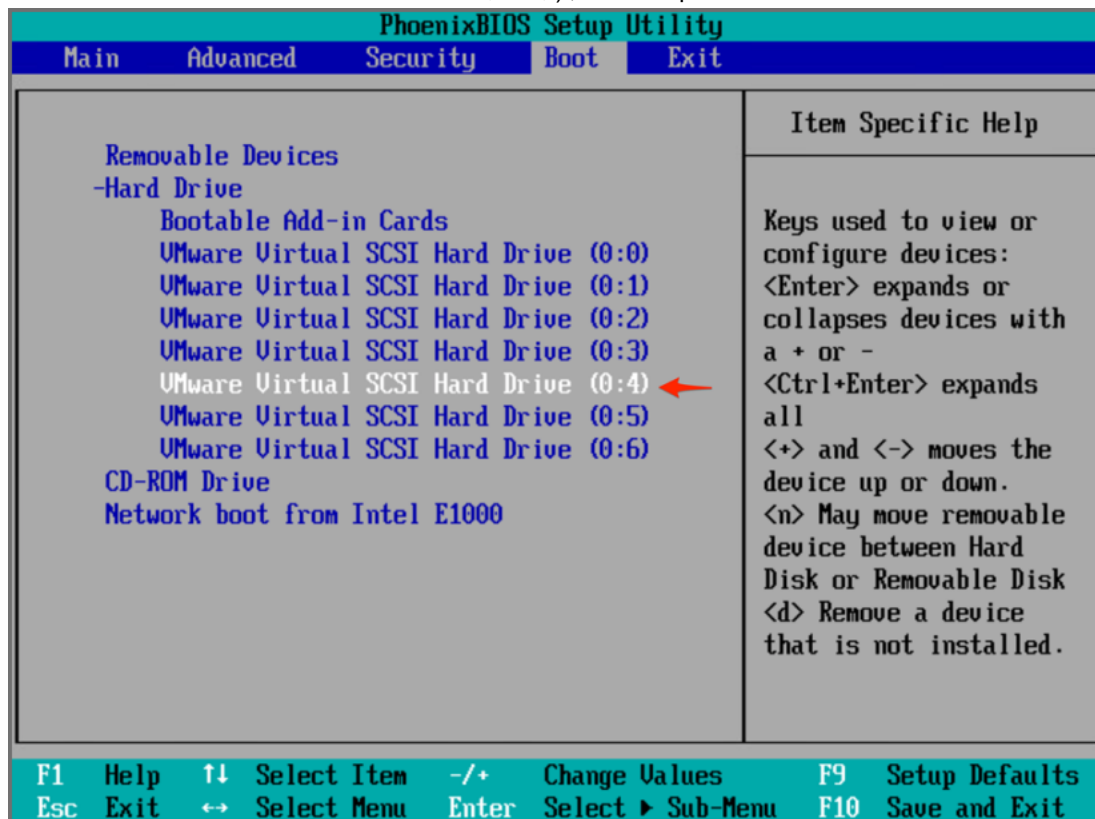
CPU		8	
Memory		24	GB
Hard disks		7 total 425 GB	
> Hard disk 1	80 GB SCSI(0:0)		
> Hard disk 2	60 GB SCSI(0:1)		
> Hard disk 3	60 GB SCSI(0:2)		
> Hard disk 4	50 GB SCSI(0:3)		
> Hard disk 5	25 GB SCSI(0:4)		
> Hard disk 6	50 GB SCSI(0:5)		
> Hard disk 7	100 GB SCSI(0:6)		
SCSI controller 0		LSI Logic Parallel	

CANCEL
OK

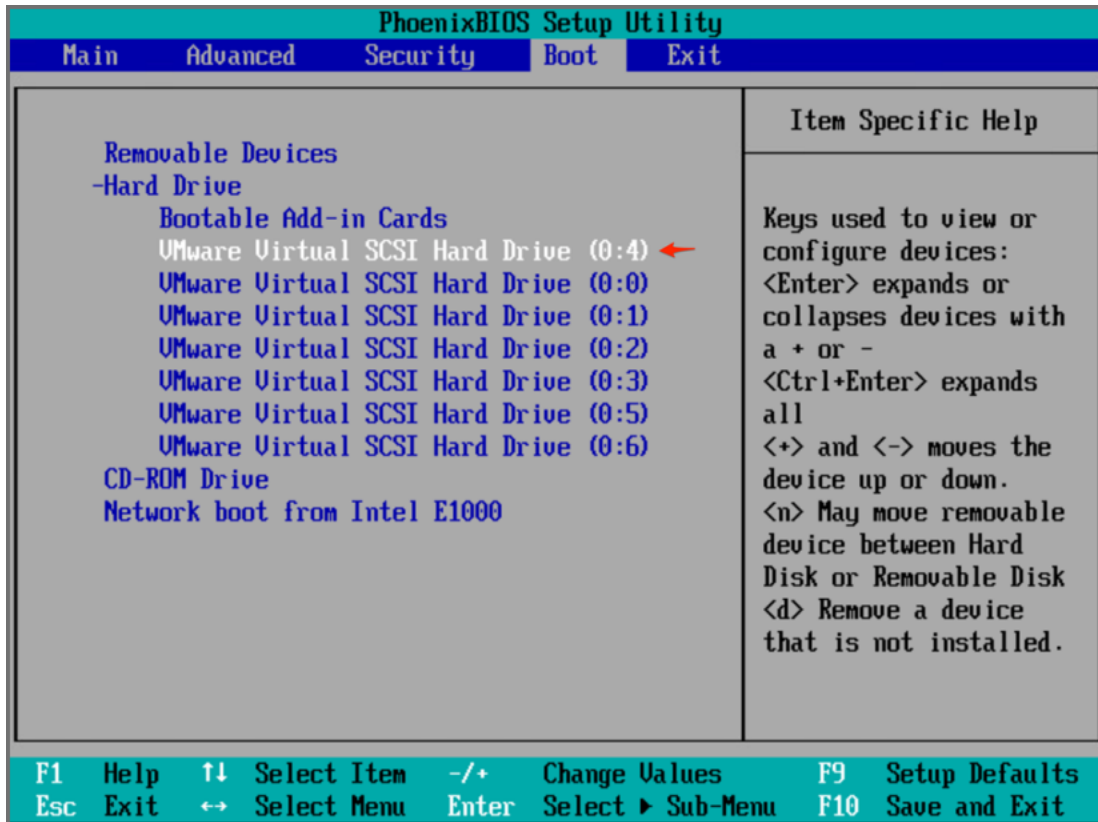
7. In the **VM Options** tab, open the **Boot Options** section.
 - a. In **Force BIOS setup**, select **During the next boot, force entry into the BIOS setup screen**.
 - b. Click **OK**.



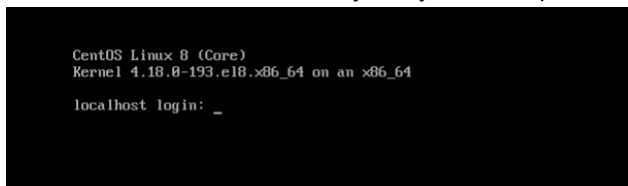
8. In VCenter, right-click the FortiSIEM VM and select **Power > Power On**.
9. In the **Summary** tab for the VM, click the **Launch Web Console** link.
The Phoenix Setup Utility will open.
10. In the Phoenix Setup Utility, use the arrow keys to go to the **Boot** tab. Identify your SCSI hard drive (in this case, VMware Virtual SCSI Hard Drive (0:4)), for example:



11. Select the new disk (in this case, VMware Virtual SCSI Hard Drive (0:4)) and use the + key to move it to the top of the list of virtual hard drives, for example:



12. Select **Save and Exit (F10)** to save your changes and exit the Phoenix Setup Utility.
13. The VM will restart automatically and you will be presented with a log in screen.



Migrate to FortiSIEM 6.1.1

Follow these steps to complete the migration process:

1. Log in to the bootloader shell as user `root` with password `ProspectHills`. You will immediately be asked to change your password.
2. Create and mount the `/images` directory:
 - a. Change directory to `root`, for example:
`cd /`
 - b. Create the `/images` directory, for example:
`mkdir -p /images`
 - c. Mount the `sdf1` (the 50GB disk) to `/images`, for example:
`mount /dev/sdf1 /images`
Or using the UUID if the disk name changed:

```
# mount -U d4a5b82f-6e73-456b-ab08-d6e6d845d1aa /images
```

```
[root@fsmshell images]# ll
total 33647324
-rw-r--r-- 1 root root      9254 Oct 28 19:42 ao_login.png
-rw-r--r-- 1 root root     4739 Oct 28 19:42 ao_upload.png
drwxr-xr-x 6 root root     4096 Oct 28 19:42 backup
-rw-r--r-- 1 root root      938 Oct 28 19:42 bg.png
-rw-r--r-- 1 root root 26843545600 Oct 26 15:00 FortiSIEM-RAW-UM-6.1.1.0118.img
-rw-r--r-- 1 root root     630081428 Oct 28 19:34 fsm_53_glassfish.xz
-rw-r--r-- 1 root root     2771411616 Oct 28 19:41 fsm_53_phoenix.xz
drwxr-xr-x 2 root root     4096 Oct 28 19:43 FSM_Bootloader_6.1.1_build0118
-rw-r--r-- 1 root root     2827940800 Oct 26 16:13 FSM_Bootloader_6.1.1_build0118.zip
-rw-r--r-- 1 root root     3926832827 Oct 26 16:19 FSM_Full_All_RAW_UM_6.1.1_build0118.zip
-rw-r--r-- 1 root root      814 Oct 26 22:26 grub_base
lrwxrwxrwx 1 root root      39 Oct 28 19:28 latest -> /images/FortiSIEM-RAW-UM-6.1.1.0118.img
-rw-r--r-- 1 root root     9254 Oct 28 19:42 login.png
drwx----- 2 root root    16384 Oct 28 19:23 lost+found
-rw-r--r-- 1 root root     169 Oct 28 19:42 network_params.json
-rw-r--r-- 1 root root     165 Oct 28 19:42 network_params.json.bak
drwxr-xr-x 2 root root     4096 Oct 28 19:42 org
-rw-r--r-- 1 root root     234 Oct 28 19:42 origdisks
-rw-r--r-- 1 root root     44 Oct 28 19:32 orig_UUID
-rwxr-xr-x 1 root root     20 Jul  8 18:15 passwd
-rw-r--r-- 1 500 501    45675 Oct 26 22:21 phoenix_config.txt
-rwxr-xr-x 1 root root     177 Oct 28 19:32 pwd_backup
-rwxr-xr-x 1 root root     56 Oct 28 19:32 pwd_backup.bak
-rw-r--r-- 1 root root     5602 Oct 28 19:42 upload.png
-rw-rw-r-- 1 500 501     125 Aug 19 18:57 VERSION
-rw-r--r-- 1 root root     3242 Oct 28 19:42 wl_login.png
-rw-r--r-- 1 root root     1114 Oct 28 19:42 wl_upload.png
[root@fsmshell images]#
```

- Run the `configFSM.sh` command to configure the migration via a GUI, for example:

```
# configFSM.sh
```

- In the first screen of the GUI select **1 Yes** to set a timezone. Press **Next**.

Configure TIMEZONE

Set TimeZone

1
Yes

2
No

< Next >
< Exit >

5. Select a region for the timezone. In this example, **US** is selected. Press **Next**.

Timezones

Select region from the menu:

↑(-)

- Australia
- Brazil
- Canada
- Chile
- Etc
- Europe
- Indian
- Mexico
- Pacific
- posix
- right
- US**

100%

< Next > < Back > < Exit >

6. Select a timezone in the selected region. In this example, **Pacific** is selected. Press **Next**.

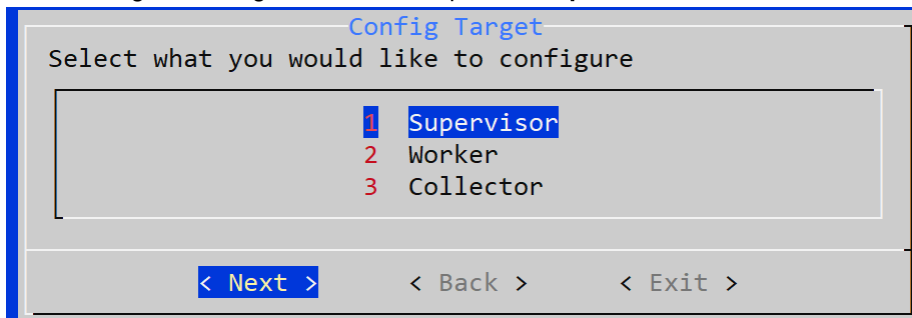
Timezones

Select your timezone in US:

Alaska	(-08:00)
Aleutian	(-09:00)
Arizona	(-07:00)
Central	(-05:00)
Eastern	(-04:00)
East-Indiana	(-04:00)
Hawaii	(-10:00)
Indiana-Starke	(-05:00)
Michigan	(-04:00)
Mountain	(-06:00)
Pacific	(-07:00)
Pacific-New	(-07:00)
Samoa	(-11:00)

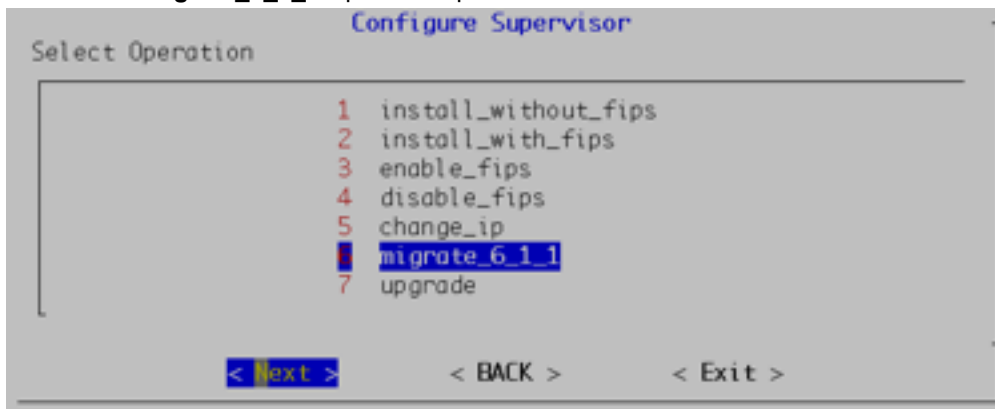
< Next > < Back > < Exit >

7. Select a target to configure. In this example, the **Supervisor** is selected. Press **Next**.



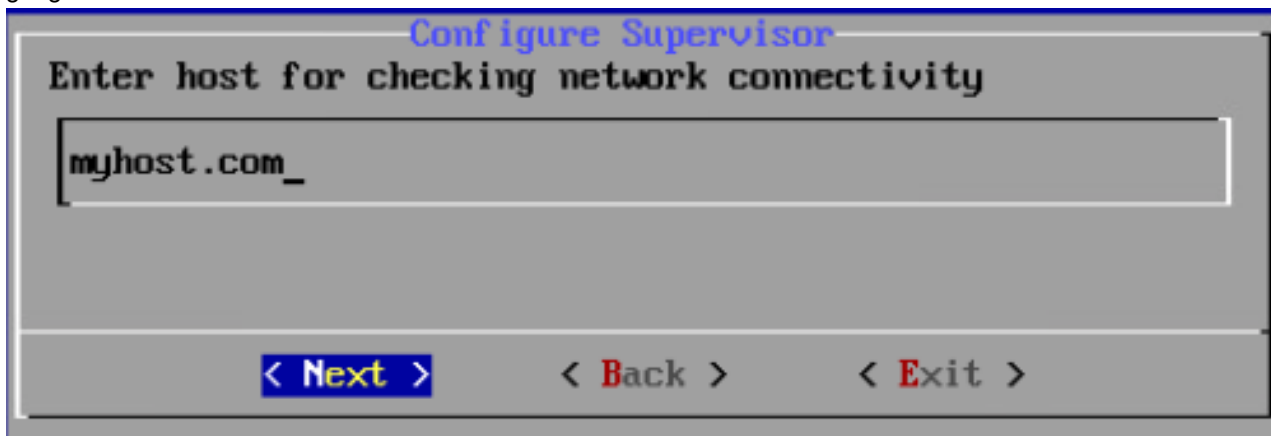
The screenshot shows a terminal window titled "Config Target". The prompt is "Select what you would like to configure". Below the prompt is a list of three options: "1 Supervisor", "2 Worker", and "3 Collector". The "1 Supervisor" option is highlighted with a blue background. At the bottom of the window, there are three navigation buttons: "< Next >", "< Back >", and "< Exit >".

8. Select the **6 migrate_6_1_1** Operation option. Press **Next**.



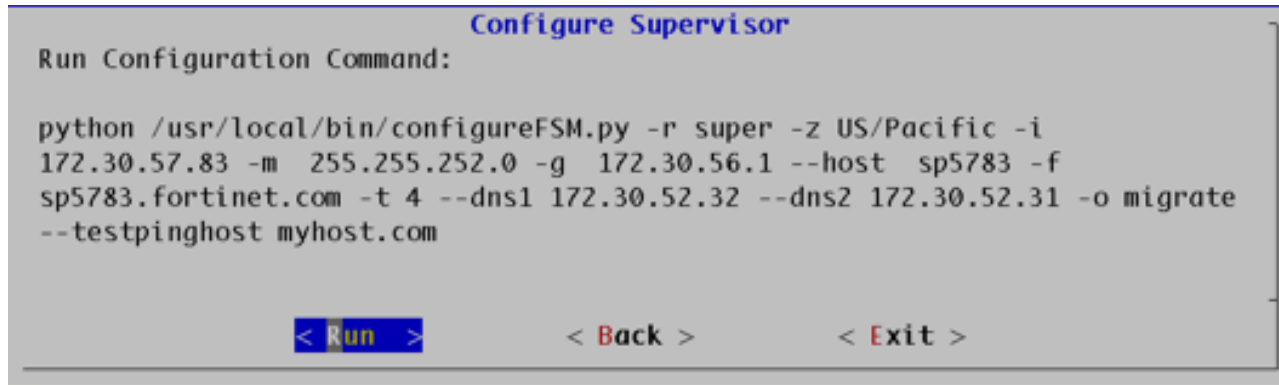
The screenshot shows a terminal window titled "Configure Supervisor". The prompt is "Select Operation". Below the prompt is a list of seven options: "1 install_without_fips", "2 install_with_fips", "3 enable_fips", "4 disable_fips", "5 change_ip", "6 migrate_6_1_1", and "7 upgrade". The "6 migrate_6_1_1" option is highlighted with a blue background. At the bottom of the window, there are three navigation buttons: "< Next >", "< BACK >", and "< Exit >".

9. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and responds to ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.



The screenshot shows a terminal window titled "Configure Supervisor". The prompt is "Enter host for checking network connectivity". Below the prompt is a text input field containing the text "myhost.com_". At the bottom of the window, there are three navigation buttons: "< Next >", "< Back >", and "< Exit >".

10. Press the **Run** command to complete migration, for example:



The options for the `configureFSM.py` script are described in the table [here](#).

11. The script will take some minutes to run. When it is finished, migration is complete.
12. To ensure `phMonitor` is running, execute the `phstatus` command, for example:
`phstatus`

Finishing Up

After successfully migrating to 6.1.1, two unmounted disks will be present in the Supervisor node.

- SDA: 80 GB: previous version root partition (unmounted).
- SDE: 50 GB: installation images (unmounted).

These are there to recover VM from a disaster or in case of an upgrade/migration failure. If everything is up and running after the upgrade or migration you can remove them from the VM.

Migrate Cluster Installation

This section provides instructions on how to migrate Supervisor, Workers, and Collectors separately in a cluster environment,

- [Delete Workers](#)
- [Migrate Supervisor](#)
- [Install New Worker\(s\)](#)
- [Register Workers](#)
- [Set Up Collector-to-Worker Communication](#)
- [Working with Pre-6.1.0 Collectors](#)
- [Install 6.1.1 Collectors](#)
- [Register 6.1.1 Collectors](#)

Delete Workers

1. Login to the Supervisor.
2. Go to **Admin > License > Nodes** and delete the Workers one-by-one.

3. Go to the **Admin > Cloud Health** page and make sure that the Workers are not present.
Note that the Collectors will buffer events while the Workers are down.
4. Shutdown the Workers.
SSH to the Workers one-by-one and shutdown the Workers.

Migrate Supervisor

Follow the steps in [Migrate All-in-one Installation](#) to migrate the supervisor node. **Note:** FortiSIEM 6.1.1 does not support Worker or Collector migration.

Install New Worker(s)

Follow the steps in [Cluster Installation > Install Workers](#) to install new Workers. You can either keep the same IP address or change the address.

Register Workers

Follow the steps in [Cluster Installation > Register Workers](#) to register the newly created 6.1.1 Workers to the 6.1.1 Supervisor. The 6.1.1 FortiSIEM Cluster is now ready.

Set Up Collector-to-Worker Communication

1. Go to **Admin > Systems > Settings**.
2. Add the Workers to the Event Worker or Query Worker as appropriate.
3. Click **Save**.

Working with Pre-6.1.0 Collectors

Pre-6.1.0 Collectors and agents will work with 6.1.1 Supervisor and Workers. You can install 6.1.1 collectors at your convenience.

Install 6.1.1 Collectors

FortiSIEM does not support Collector migration to 6.1.1. You can install new 6.1.1 Collectors and register them to 6.1.1 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. Follow these steps:

1. Copy the http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector.
2. Disconnect the pre-6.1.1 Collector.
3. Install the 6.1.1 Collector with the old IP address by the following the steps in [Cluster Installation > Install Collectors](#).
4. Copy the saved http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector to the 6.1.1 Collector.

This step is needed for Agents to work seamlessly with 6.1.1 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.1 migration, this password is lost.

Register 6.1.1 Collectors

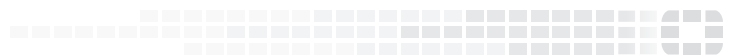
Follow the steps in [Cluster Installation > Register Collectors](#), with the following difference: in the `phProvisionCollector` command, use the `--update` option instead of `--add`. Other than this, use the exactly the same parameters that were used to register the pre-6.1.1 Collector. Specifically, use this form of the

`phProvisionCollector` command to register a 6.1.1 Collector and keep the old associations:

```
# /opt/phoenix/bin/phProvisionCollector --update <user> '<password>' <Super IP or Host>
    <Organization> <CollectorName>
```

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

Re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.